PCT/EP2004/008591

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

June 16, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.
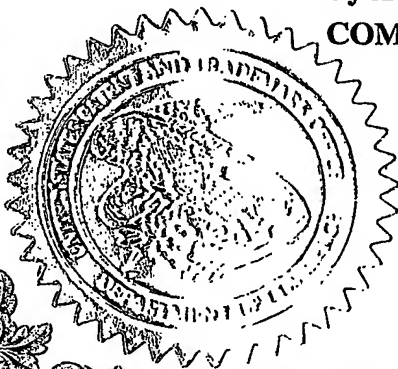
APPLICATION NUMBER: *60/491,584*
FILING DATE: *July 31, 2003*

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

E. BORNETT
Certifying Officer

Please type a plus sign (+) inside this box ⟶ [+]

PROVISIONAL APPLICATION FOR PATENT COVER SHEET
This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Rogier August Casper Joseph	Noldus	Tilburg, The Netherlands

[ ] Additional inventors are being named on the ____ separately numbered sheets attached hereto

TITLE OF THE INVENTION (280 characters max)

IMEI verification using SCP instead of MSC

CORRESPONDENCE ADDRESS

Direct all correspondence to:

[✔] Customer Number | 27045

OR

Type Customer Number here

Place Customer Number Bar Code Label here

[ ] Firm or Individual Name	
Address	
Address	
City		State		ZIP	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS (check all that apply)

[✔] Specification *Number of Pages* | 8

[✔] Drawing(s) *Number of Sheets* | 0

[✔] Application Data Sheet. See 37 CFR 1.76

[ ] CD(s), Number

[ ] Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

[ ] A check or money order is enclosed to cover the filing fees

[✔] The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number | 50-179

[ ] Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($)

$160.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

[ ] No.

[ ] Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME John C. Han

TELEPHONE (972) 583-7686

Date | 07/31/2003

REGISTRATION NO. | 41,542
(if appropriate)

Docket Number: | P18278-US1

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.   P18LARGE/REV05

Application Data Sheet

Application Information

Application Type::	Provisional
Subject Matter::	Utility
Title – Line One::	IMEI verification using SCP instead of MSC
Attorney Docket Number::	P18278-US1
Total Drawing Sheets::	0
Small Entity::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority type::	Inventor
Primary Citizenship Country::	The Netherlands
Status::	Full Capacity
Given Name::	Rogier August Casper Joseph
Family Name::	Noldus
Name Suffix::	
City of Residence::	Tilburg
State or Province of Residence::	
Country of Residence::	The Netherlands
Street of mailing address::	Naardenstraat 46
City of mailing address::	Tilburg
State or Province of mailing address::	
Country of mailing address::	The Netherlands
Postal or Zip Code of mailing address::	5045 ML

Correspondence Information

Correspondence Customer Number::	27045
Phone Number::	972-583-7686
Fax Number::	972-583-7864

E-Mail Address::   john.han@ericsson.com

Representative Information

Representative Customer Number::   27045

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::

Foreign Priority Information

Country::	Application Number::	Filing Date::	Priority Claimed::

Assignment Information

Assignee Name::   Telefonaktiebolaget LM Ericsson (publ)

State or Province of mailing address::   Stockholm

Country of mailing address::   Sweden

Postal or Zip Code of mailing address:: S-126 25

IMEI V rification

1. Current Situation

Telecommunication Network Operators and consumers are faced with the problem of GSM handset theft. Regulators are looking for means to curb handset theft. One means of curbing theft is ensuring that stolen handset cannot be used.

Although both the SIM card and the Mobile Station (MS = GSM handset) can be protected by means of a security code, it may occur that neither SIM nor MS is protected.

The International Mobile Equipment Identifier (IMEI) is a code that is programmed into an MS and that uniquely identifies the MS. The IMEI may be accompanied by a Software Version (SV); the combination of IMEI and SV is referred to as IMEISV. Refer to figures 1 and 2 for the structure of the IMEI and IMEISV.
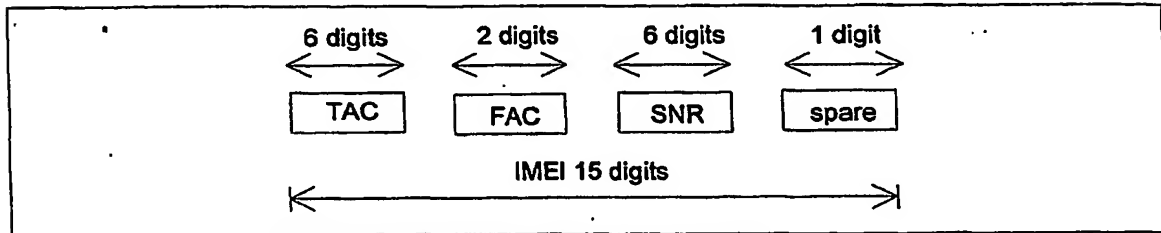

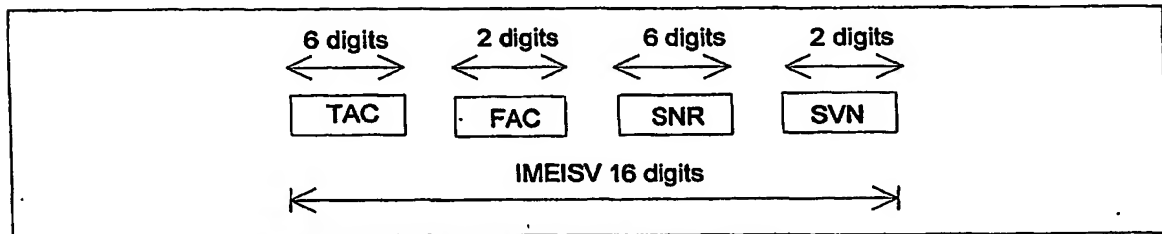Figure 1: Structure of IMEI (source: 3GPP)

Figure 2: Structure of IMEISV (source: 3GPP)

When an MS is reported as stolen, the IMEI of that MS may be included in a "blacklist" in the Equipment Identification Register (EIR). Each operator may have one or more EIRs in its network.

When a subscriber registers in an MSC, the MSC may be configured to query the EIR of the PLMN where the subscriber belongs to. The purpose of this query is to ascertain whether the MS used by the subscriber is on a "blacklist" or a "greylist". If so, then registration of the MS will be disallowed by the MSC or may be subject to tracing. Refer to 3GPP TS 22.016 [1] for usage of EIR and IMEI. GSM Association's Permanent Reference Document (PRD) TW06 [2] explains the functionality of the EIR. The structure of the IMEI is specified in 3GPP TS 23.003 [5].

2. Problem definition

The method of having the MSC query the EIR of the HPLMN of the served subscriber has the following disadvantages:

- Once a subscriber has registered with an MSC and does not perform a Location Update after registration, then the MSC will not query the EIR when the MS is switched off and subsequently on. (This is MSC configuration dependent.)

- When a subscriber is detached from an MSC and subsequently re-attaches to that MSC, the subscriber may have changed the SIM from one MS to another; this may not be noticed by the MSC.

- The MSC can be configured with a single EIR Address only.

3. Solution

Because of the drawbacks of MSC-based IMEI verification, the current invention proposes to have the SCP (Service Control Point) perform IMEI verification. The SCP-based IMEI verification can be considered to complement the MSC-based verification.

In CAMEL Phase 4 (which is part of the 3GPP Rel-5 Mobile Network specifications), mechanisms are introduced to transport the IMEI of the served subscriber from the MSC to the SCP. These mechanisms are:

(1) CAMEL Service Invocation: when the served subscriber initiates a call or non-call activity, then the MSC includes the IMEI of the MS in the CAMEL Service Invocation. The protocol used between the MSC and the SCP is *CAP V4*. CAP V4 contains the IMEI of the MS used by the served subscriber.

(2) The SCP can query the MSC for the IMEI of the MS used by a subscriber. The SCP sends the query to the HLR; the HLR passes the query on to the MSC where the subscriber is registered. The MSC retrieves the IMEI from the MS. The MSC needs to set up radio contact with the MS, in order to obtain the IMEI.

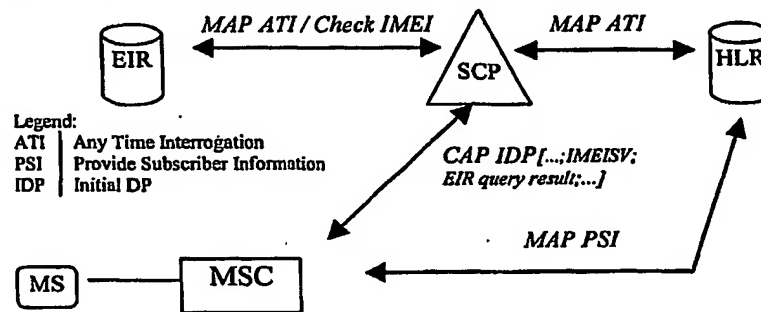These existing mechanisms may be used to verify the IMEI by the SCP. Refer to figure 3.

MAP ATI / Check IMEI EIR SCP *MAP ATI* HLR

Legend:
ATI | Any Time Interrogation
PSI | Provide Subscriber Information
IDP | Initial DP

CAP IDP[...;IMEISV; EIR query result;...]

MAP PSI

MS — MSC

Figure 3: IMEI query by SCP

The following scenarios illustrate how the solution can be applied in various situations. However, other scenarios and implementations are possible.

Scenario 1: Mobile Originated call set up

When a subscriber sets up a Mobile Originated (MO) call, the MSC initiates contact with the SCP. The SCP receives the CAP Initial DP (IDP) operation. IDP contains the IMEI of the MS used by the subscriber.

The SCP uses the MAP Any Time Interrogation (ATI) message to query the EIR. The EIR returns an indication to the SCP, whether the IMEI of the subscriber is on a blacklist.

If the EIR indicates to the SCP that the IMEI is not on a blacklist, then the SCP allows the call to continue. Otherwise, the call will not be allowed; the SCP shall then take appropriate action.

Scenario 2: Mobile Originated Short Message Service

When a subscriber submits a Short Message, the MSC initiates contact with the SCP. The SCP receives the CAP Initial DP SMS (IDP SMS) operation. IDP SMS contains the IMEI of the MS used by the subscriber.

3

The SCP uses the MAP ATI message to query the EIR. The EIR returns an indication to the SCP, whether the IMEI of the subscriber is on a blacklist.

If the EIR indicates to the SCP that the IMEI is not on a blacklist, then the SCP allows the SMS submission to continue. Otherwise, the SMS submission will not be allowed; the SCP shall then take appropriate action.

Scenario 3: GPRS PDP Context set up

When a subscriber establishes a GPRS Packet Data Protocol (PDP) Context, the SGSN initiates contact with the SCP. The SCP receives the CAP Initial DP GPRS (IDP GPRS) operation. IDP GPRS contains the IMEI of the MS used by the subscriber.

The SCP uses the MAP ATI message to query the EIR. The EIR returns an indication to the SCP, whether the IMEI of the subscriber is on a blacklist.

If the EIR indicates to the SCP that the IMEI is not on a blacklist, then the SCP allows the PDP Context establishment to continue. Otherwise, the PDP Context establishment will not be allowed; the SCP shall then take appropriate action.

Scenario 4: Mobile-to-Mobile call set up

When a subscriber sets up a MO call, the MSC initiates contact with the SCP. The SCP deduces that the destination subscriber belongs to the same PLMN. The SCP uses MAP ATI to retrieve the IMEI of the MS used by the destination subscriber. When the SCP has obtained the IMEI, the SCP queries the EIR.

If the EIR indicates that the MS of the destination subscriber is on a blacklist, then the SCP disallows the call to that subscriber and takes appropriate action.

As an alternative to using MAP ATI between the SCP and the EIR, the MAP Message *Check IMEI* may be used. Table 1 shows a comparison between the use of MAP ATI and the use of MAP Check IMEI, for the purpose of IMEI verification by the SCP.

Table 1: comparison between ATI and Check IMEI

MAP ATI	MAP Check IMEI
Support of MAP ATI is already specified for SCP, but needs to be enhanced for usage to EIR.	Support of MAP Check IMEI is not yet specified for SCP.
Support of MAP ATI is not yet specified for the EIR.	Support of MAP Check IMEI is already specified for the EIR.
MAP ATI between SCP and EIR may be used to EIR in HPLMN only. Hence, it can not be used for subscribers from other PLMNs.	If SCP supports MAP Check IMEI, then it may potentially be used to EIRs from any PLMN. Hence, it may be used for subscribers from other PLMNs.

Table 1 reveals that the usage of MAP Check IMEI has advantages over the use of MAP ATI.

As an implementation example, when Check IMEI is used, an MSC may invoke a *Serving Network based Dialled Service* for all outgoing calls, or for outgoing calls that satisfy certain trigger criteria. Serving Network based Dialled Services do not require a subscription. The Service that is invoked may use MAP Check IMEI to the EIR of the PLMN of the calling subscriber; this EIR may be located in any PLMN.

In this manner, an operator can activate a feature in selected MSCs, to check the IMEI of all served subscribers.

There are many other call scenarios whereby an SCP-based service may be utilised to verify the IMEI of a served subscriber. The principle may be used for Circuit Switched (CS) terminals and for Packet Switched (PS) terminals.

4

The EIR of an operator may be connected to the Central Equipment Identity Register (CEIR), operated by the GSM Association. The CEIR maintains IMEI lists of all operators that join the CEIR. The EIR may update itself with information stored in the CEIR.

3GPP TS 29.002 [3] specifies *"The EIR address is either unique or could be d riv d from the IMEI. The type of address is not defined."*. Hence, when the SCP has to query the EIR, it may analyse the IMEI and determine whether it shall query an EIR resulting from the IMEI or a pre-defined EIR (e.g. its own EIR).

SCP-based IMEI verification may be considered a *complement* to the MSC-based IMEI verification, as opposed to being a *replacement* thereof. However, the capabilities of an SCP, w.r.t. IMEI verification, are more extensive than the capabilities of an MSC in this regard.

To prevent that both an MSC and an SCP check the IMEI of a served subscriber, the information flow between MSC and SCP used for IN Service invocation, may contain an indication whether MSC-based IMEI verification has taken place and if so, the result of this verification. If the MSC indicates to the SCP that IMEI verification has been executed already, then SCP may omit its IMEI verification for this call. This is depicted by *"CAP IDP[...; IMEISV; EIR query result; ...]"* in figure 3. See also underneath a possible enhancement of the CAP syntax (for call control), as specified in 3GPP TS 29.078 [6] (parameter "iMEIQueryresult" is added).

```
< start of extract from 3GPP TS 29.078 >

InitialDPArg {PARAMETERS-BOUND : bound} ::= SEQUENCE {

    initialDPArgExtension          [59] InitialDPArgExtension {bound}         OPTIONAL,
    ...
    }

InitialDPArgExtension {PARAMETERS-BOUND : bound} ::= SEQUENCE {
    gmscAddress                    [0] ISDN-AddressString                    OPTIONAL,
    forwardingDestinationNumber    [1] CalledPartyNumber {bound}             OPTIONAL,
    ms-Classmark2                  [2] MS-Classmark2                         OPTIONAL,
    iMEI                           [3] IMEI                                  OPTIONAL,
    supportedCamelPhases           [4] SupportedCamelPhases                  OPTIONAL,
    offeredCamel4Functionalities   [5] OfferedCamel4Functionalities          OPTIONAL,
    ..._
    iMEIQueryresult                [6] IMEIQueryresult                       OPTIONAL
}
< end of extract from 3GPP TS 29.078 >
```

3.1 Early UMTS Equipment verification

As an extension, the following may be considered. In the 3GPP Rel-5 specifications, the principle is introduced that the IMEISV is used to query a HPLM-located data base. This data base contains a list with "Early UMTS Equipment" (Early UE), identified by IMEISV. For some Early UE's, problems have been identified that relate to that Early UE's capability in the Radio Access Network. The Early UE data base marks per IMEISV which problems are known to the UE identified with that IMEISV. When an MSC queries the Early UE Database, it may take special pre-caution for handling that call, based on the reported problems of that IMEISV.

Refer to 3GPP TR 25.994 [4] for a list of the Early UE problems that may be listed and reported.

Since the Early UE database is located in HPLMN, it is not possible for the MSC to perform this query for inbound roaming subscribers. The address of the Early UE database belonging to the inbound roaming subscriber, is not known to the MSC. Hence, the gsmSCF of that inbound roaming subscriber, which handles a CAMEL service for that subscriber, may perform this query. According to current art, the IMEISV is reported in the CAMEL Service invocation request. The gsmSCF uses the reported IMEISV to perform the query. The result of that query may be used by the gsmSCF to adapt its service behaviour, based on the reported problems of that IMEISV. Refer to figure 4 for a graphical presentation of this principle.
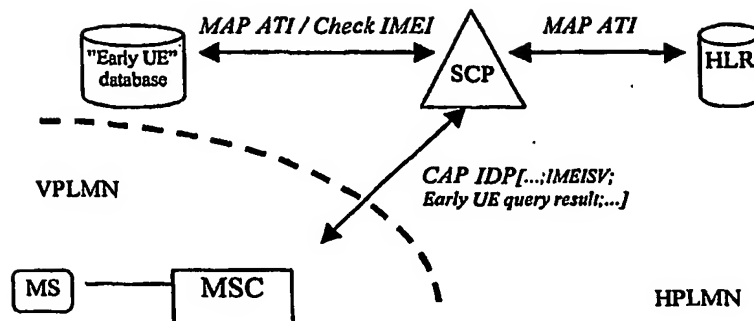
Figure 4: Early UE verification by gsmSCF

As a further enhancement to the above-proposed principle (Early UE verification by gsmSCF), the following may be considered. When the MSC has successfully queried Early UE database (in the case that subscriber is in HPLMN), then the result of this database query may be reported to the gsmSCF, in the CAMEL Service invocation. In that way, the gsmSCF can adapt its service behaviour, as described above, without having to execute the database query. This is depicted by "*CAP IDP[...; IMEISV; Early UE query result; ...]*" in figure 4. See also underneath a possible enhancement of the CAP syntax (for call control), as specified in 3GPP TS 29.078 [6] (parameter "equipmentStatus" is added). The proposed encoding equipmentStatus is in accordance with the encoding of equipmentStatus in 3GPP TS 29.002 [3].

```
< start of extract from 3GPP TS 29.078 >

InitialDPArg {PARAMETERS-BOUND : bound} ::= SEQUENCE {

     initialDPArgExtension          [59] InitialDPArgExtension {bound}          OPTIONAL,
     ...
     }


InitialDPArgExtension {PARAMETERS-BOUND : bound} ::= SEQUENCE {
     gmscAddress                    [0]  ISDN-AddressString                     OPTIONAL,
     forwardingDestinationNumber    [1]  CalledPartyNumber {bound}              OPTIONAL,
     ms-Classmark2                  [2]  MS-Classmark2                          OPTIONAL,
     iMEI                           [3]  IMEI                                   OPTIONAL,
     supportedCamelPhases           [4]  SupportedCamelPhases                   OPTIONAL,
     offeredCamel4Functionalities   [5]  OfferedCamel4Functionalities           OPTIONAL,
     ...
     equipmentStatus                [6]  EquipmentStatus                        OPTIONAL
     }


EquipmentStatus ::= ENUMERATED {
     whiteListed       (0),
     blackListed       (1),
     greyListed        (2)}

< end of extract from 3GPP TS 29.078 >
```

The Early UE verification by gsmSCF may be used in combination with call control, SMS control and GPRS control. It may also be used during non-call/SMS/GPRS related service processing.

The implementation of the Early UE query by gsmSCF may be aligned with the implementation of the IMEI check by gsmSCF. I.e. the same MAP Message may be used for these purposes. The protocol details regarding the information flow between gsmSCF and Early UE database require further investigation.

4. Glossary

ATI	Any Time Interrogation
CAMEL	Customised Applications for Mobile network Enhanced Logic
CAP V4	CAMEL Application Part Version 4
CS	Circuit Switched
CEIR	Central Equipment Identification Register
EIR	Equipment Identification Register
3GPP	3rd Generation Partnership Project
GPRS	General Packet Radio System
GSM	Global System for Mobile Communication
HLR	Home Location Register
IMEI	International Mobile Equipment Identifier
IMEISV	IMEI + Software Version
MAP	Mobile Application Part
MS	Mobile Station
MSC	Mobile Services Switching Centre
(H)PLMN	(Home) Public Land Mobile Network (e.g. GSM network)
PDP	Packet Data Protocol
PS	Packet Switched
SCF	Service Control Function
SCP	Service Control Point
SIM	Subscriber Identity Module
SGSN	Serving GPRS Support Node
SMS	Short Message Service
UE	UMTS Equipment
UMTS	Universal Mobile Telecommunication System

5. References

[1]	3GPP TS 22.016; "International Mobile Equipment Identities (IMEI)"
[2]	GSMA PRD TW06; "IMEI Allocation and Approval Guidelines".
[3]	3GPP TS 29.002; "Mobile Application Part"
[4]	3GPP TR 25.994; "Measures employed by the UMTS Radio Access Network (UTRAN) to overcome early User Equipment (UE) implementation faults"

[5]	3GPP TS 23.003; "Numbering, addressing and Identification"
[6]	3GPP TS 29.078, CAMEL Application Part

The above documents can be obtained at: http://www.3gpp.org/

For information on the CEIR, the following URLs may be used:

http://www.gsmworld.com/news/press_2002/press_22.shtml

http://www.gsmworld.com/using/security/index.shtml

http://www.gsmworld.com/documents/twg/tw06320.pdf